A chaotic image encryption scheme owning temp-value feedback

Leo Yu Zhang[a,*], Xiaobo Hu[a], Yuansheng Liu[b], Kwok-Wo Wong[c], Jie Gan[a]

[a] *State Grid Electric Power Research Institute, Qinghe, Beijing 100192, China*
[b] *College of Information Engineering, Xiangtan University, Xiangtan 411105, Hunan, China*
[c] *Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China*

Abstract

This paper presents a novel efficient chaotic image encryption scheme, in which the temp-value feedback mechanism is introduced to the permutation and diffusion procedures. Firstly, a simple trick is played to map the plain-image pixels to the initial condition of the Logistic map. Then, a pseudorandom number sequence (PRNS) is obtained from iterating the map. The permutation procedure is carried out by a permutation sequence which is generated by comparing the PRNS and its sorted version. The diffusion procedure is composed of two reversely executed rounds. During each round, the current plain-image pixel and the last cipher-image pixel are used to produce the current cipher-image pixel with the help of the Logistic map and a pseudorandom number generated by the Chen system. To enhance the efficiency, only expanded XOR operation and modulo 256 addition are employed during diffusion. Experimental results show that the new scheme owns a large key space and can resist the differential attack. It is also efficient.

Keywords: image encryption, Chen system, Logistic map, permutation, diffusion

1. Introduction

In the information era, digital images have been widely used for various applications, such as entertainment, business, health service and military affairs, etc. All the sensitive data should be encrypted before transmission to avoid eavesdropping. However, bulk data size and high redundancy among the raw pixels of a digital image make the traditional encryption algorithms, such as DES, IDEA, AES, not able to be operated efficiently. Therefore, designing specialized encryption algorithms for digital images has attracted much research effort. Some intrinsic properties of chaotic systems, such as ergodicity, sensitive to the initial condition and control parameters, are analogous to the confusion and diffusion properties designed by Shannon [1]. Thus makes it natural to employ chaotic systems in image encryption algorithms [2–10]. Meanwhile, the art of deciphering has also made new achievements in the last few decades. Some of the existing image encryption algorithms are found insecure [11–18] to different degrees due to the following defects: 1) the (equivalent) secret key can be obtained by the brute-force attack due to the dynamical degradation of chaotic systems in digital domain; 2) all the operations employed in the encryption process are reversible or even linear, therefore the mathematical model of the scheme is not a keyed

*Corresponding author.
Email address: leoxtu@gmail.com (Leo Yu Zhang)

one-way function [19]. In [20], some basic requirements for evaluating the chaotic image encryption algorithm are concluded.

The permutation-diffusion structure becomes the basis of many chaotic image encryption schemes since Fridrich developed a chaos-based image encryption scheme of this structure in 1998 [2]. The symmetric image encryption scheme in [4] extended the Cat map to three-dimensional to make it suitable for permutation in space and followed the similar diffusion construction of Fridrich's. In 2004, Mao et al. proposed an image encryption algorithm, where the discrete Baker map was employed for permutation [8]. It's worth mentioning that most image encryption schemes of this structure have to execute the permutation and diffusion procedures alternatively several rounds to fulfill the security requirement, which will certainly lead to some reduction in efficiency. Nonetheless, Solak et al. proposed a chosen ciphertext attack in 2010 by utilizing the relationship between the pixels in the neighboring encryption rounds [12]. This attack is efficient to Fridrich's scheme [2] and it can also be applied to Chen's scheme [4]. In addition, it is reported in [21] that the equivalent key of several permutation-diffusion image ciphers, such as the schemes suggested in [2, 4, 8, 22], can be recovered when only one iteration round is applied.

Meanwhile, image encryption algorithms of other structures have also been developed. In 2010, Patidar et al. suggested a substitution-diffusion structure for color image [10], which was attacked in [18]. In [9], Huang et al. presented a multi-chaotic system based permutation scheme [9], in which pixel positions and bits in the individual pixel are shuffled together to achieve permutation and substitution simultaneously. Intuitively, permutation-only schemes are not secure against known/chosen plaintext attack. In [13, 17], Li et al. proposed the quantitative and optimal quantitative cryptanalysis of the permutation-only encryption schemes with respect to known/chosen plaintext attack.

By combining the Chen system and the Logistic map, a novel permutation-diffusion image encryption algorithm is given in this paper. To resist the known attacks and achieve better efficiency, two temp-value feedback mechanisms are imbedded into a single permutation-diffusion round. In the permutation part, we develop different permutation sequences for different plain-images by means of mapping some information of the plain-image to the generation process of the permutation sequence. Thus makes the permutation acts in a "one time pad" manner. In the diffusion part, another feedback technique is employed to make the equivalent key generation depend on both the plain-image and the temp-value. By combining the proposed permutation and diffusion technique, the scheme frustrates the known attacks [12, 21]. In addition, we add a reversely executed diffusion process to make the scheme sensitive to changes of plain-image.

The rest of this paper is organized as follows. Section 2 presents some descriptions of the prerequisites of the algorithm, such as expanded XOR operation, the temp-value feedback mechanism, followed by the detailed encryption/decryption procedures. In Sec. 3, we evaluate the new scheme via numerical simulations and comparisons. The last section gives some concluding remarks.

2. The proposed image encryption algorithm

2.1. The involved chaotic systems

Chen system has been widely adopted in many chaotic image encryption algorithms, it can be modeled by [4]

$$\begin{cases} \dot{\mathrm{x}} = a(y - x), \\ \dot{\mathrm{y}} = (c - a)x - xz + cy, \\ \dot{\mathrm{z}} = xy - bz, \end{cases} \tag{1}$$

where a, b and c are system parameters. When $a = 35$, $b = 3$ and $c \in [20, 28.4]$, the system is chaotic. In the proposed encryption algorithm, c is fixed at 28.

The other chaotic system employed in this encryption algorithm is the Logistic map

$$y_{n+1} = \mu \cdot y_n \cdot (1 - y_n),$$

where $y_n \in (0, 1)$ and μ is the control parameter. When $\mu \in (3.5699456, 4)$, the output sequence is ergodic in the unit interval $(0, 1)$, which makes the Logistic map suitable for pseudorandom number generation [23].

2.2. The expanded XOR *operation*

The expanded XOR (eXOR) operation is introduced to enhance the whole security level of the scheme. For two inputs $x = \sum_{i=0}^{7} x_i$ and $r = \sum_{i=0}^{8} r_i$,

$$\text{eXOR}(x, r) = \sum_{i=0}^{7} not(x_i \oplus r_i \oplus r_{i+1}) \cdot 2^i,$$

where $not(x)$ flips a single bit x. Then one can deduce a property of eXOR as follows.

Property 1. *If the equation*

$$\text{eXOR}(x, r) = t$$

holds, then

$$\text{eXOR}(t, r) = x.$$

Proof. This property can be proved by checking every bit of $\text{eXOR}(x, r)$ and $\text{eXOR}(t, r)$, which is given in table 1.

Table 1: The result of $not(x_i \oplus r_i \oplus r_{i+1})$.

x_i	$r_i r_{i+1}$			
	00	01	10	11
0	1	0	0	1
1	0	1	1	0

□

2.3. The temp-value feedback mechanism

The core of the proposed encryption algorithm, two feedback techniques called plaintext feedback in permutation and plaintext/ciphertext feedback in diffusion, will be introduced in the following sections.

2.3.1. Plaintext feedback in permutation

Permutation is a basic component of both traditional and chaos-based encryption algorithms. In the traditional encryption schemes, such as DES and AES, the permutation tables employed are fixed during designing. While most chaos-based schemes, such as the schemes in [2, 4, 5, 8], apply key-dependent permutation sequence. But all of them have one feature in common: the permutation sequences (tables) are fixed once the secret key is given. By introducing the plaintext feedback technique, we develop a new approach to design dynamic permutation sequence, i.e., different plain-images corresponding to different permutation sequences, thus makes permutation executes in a "one time pad" manner. The basic process of our method can be described as follows.

Without loss of generality, denote an 8-bit sequence and its permutated version by $\{a_i\}_{i=1}^n$ and $\{a'_i\}_{i=1}^n$, respectively. For any $i \in \{1, 2, \cdots, n\}$, permutation only makes change to the position of a_i while keeps its value fixed, then one has

$$\max(a_i) = \max(a'_i),$$
$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} a'_i.$$

Set

$$y_0 = \begin{cases} 0, & \text{if } \max(a_i) = 0, \\ \frac{\sum_{i=1}^n a_i}{n \cdot \max(a_i)} = \frac{\sum_{i=1}^n a'_i}{n \cdot \max(a'_i)}, & \text{otherwise,} \end{cases} \tag{2}$$

Note that $y_0 = 0$ or $y_0 = 1$ if and only if $a_i \equiv c$, where $i \in \{1, 2, \cdots, n\}$ and c is a constant, the permutation can be simply ignored when this situation occurs during encryption. Iterate a nonlinear function $y_i = f(y_{i-1}, u)$ from y_0 for n times to obtain a PRNS $\{y_i\}_{i=1}^n$. Then a permutation sequence $\{s_i\}_{i=1}^n$ is derived by comparing $\{y_i\}_{i=1}^n$ and its sorted version, where y_{s_i} is the i-th largest element in the sequence $\{y_i\}_{i=1}^n$. To get the permutated sequence $\{a'_i\}_{i=1}^n$, simply set

$$a'_i = a_{s_i}.$$

It should be noticed that the inverse permutation shares the same structure of the original one because Eq. (2) always holds. In the proposed permutation, some information of the original sequence $\{a_i\}_{i=1}^n$ is mapped to the initial value of the nonlinear function. Then one can develop different permutation sequences $\{s_i\}_{i=1}^n$ for different plain-images. Thus makes this kind of permutation tough for the known/chosen plaintext attack proposed in [13, 17]. In the suggested encryption algorithm, the Logistic map serves as the nonlinear function and its parameter μ is considered as part of the secret key. For the sake of larger key space, one can employs nonlinear function with more control parameters after careful study.

2.3.2. Plaintext/ciphertext feedback in diffusion

The diffusion procedure presented in this scheme is composed of two rounds, which are denoted by *Diffusion I* and *Diffusion II*, respectively. In *Diffusion I*, we first calculate the equivalent secret keys according to the gray value of the last plain-image pixel. Then the current cipher-image pixel can be obtained by combining the current plain-image pixel, the last cipher-image pixel and the current equivalent keys together with the help of the above mentioned eXOR operation and modulo 256 addition. Namely, each pair of equivalent keys are produced by using the plaintext feedback technique and every cipher-image pixel is calculated by using the ciphertext feedback

technique. *Diffusion II* owns the same structure as *Diffusion I* but execute reversely, thus makes the diffusion procedure sensitive to changes of plain-image. Suppose an 8-bit PRNS $\{x_i\}_{i=0}^{n+3}$ is available, one can compute the cipher-image pixel sequence $\{c_i\}_{i=1}^{n}$ from $\{p_i\}_{i=1}^{n}$ as follows.

- *Diffusion I*: Set $p_0 = x_n$, $m_0 = x_{n+1}$ and $i = 1$, get $\{m_i\}_{i=1}^{n}$ by the following steps.
  - Obtain the initial condition r_0 of the Logistic map by

$$r_0 = \begin{cases} (x_{i-1} + 127)/(p_{i-1} + 255), & \text{if } x_{i-1} \le p_{i-1}, \\ (p_{i-1} + 127)/(x_{i-1} + 255), & \text{otherwise.} \end{cases} \tag{3}$$

  - Iterate the Logistic map twice from r_0 to obtain $\hat{r}$ and $\hat{r}'$, refresh them with Eq. (4) and denote the result by r and r', respectively.

$$g(x) = \lfloor x \cdot 10^8 \rfloor \bmod 512, \tag{4}$$

    where $\lfloor x \rfloor$ returns the nearest integers smaller than or equal to x.
  - Compute m_i by

$$m_i = \mathrm{eXOR}(p_i, r) \dot{+} \mathrm{eXOR}(m_{i-1}, r'), \tag{5}$$

    where $a \dot{+} b = (a + b) \bmod 256$.
  - Let $i = i + 1$, execute the above three steps for $n - 1$ more times and get $\{m_i\}_{i=1}^{n}$.
- *Diffusion II*: Similar to *Diffusion I*, one can obtain $\{c_i\}_{i=1}^{n}$ by diffuse $\{m_i\}_{i=1}^{n}$ in a reverse order. Set $m_{n+1} = x_{n+3}$, $c_{n+1} = x_{n+2}$, for $i = n \sim 1$, *Diffusion II* is the same as *Diffusion I* except Eq. (3) and Eq. (5) are replaced by

$$r_0 = \begin{cases} (x_{n-i} + 127)/(m_{i+1} + 255), & \text{if } x_{n-i} \le m_{i+1}, \\ (m_{i+1} + 127)/(x_{n-i} + 255), & \text{otherwise,} \end{cases}$$

  and

$$c_i = \mathrm{eXOR}(m_i, r) \dot{+} \mathrm{eXOR}(c_{i+1}, r'), \tag{6}$$

  respectively.

2.4. Encryption algorithm

Combining the above mentioned two kinds of temp-value feedback techniques, a novel symmetric gray image encryption scheme is presented in this section. Without loss of generality, one can scan a plain-image in the raster order and represent it as a one-dimensional 8-bit sequence $\{p_i\}_{i=1}^{n}$. Given the secret key $\boldsymbol{K} = (x, y, z, \mu)$, where (x, y, z) is the initial conditions of the Chen system and $\mu \in (3.5699456, 4)$ is the control parameter of the Logistic map, the details of the encryption procedure are described as follows.

- *Step (1) Initialization*: Implement the Chen system (1) with the fourth-order Runge-Kutta method of step length $h = 0.001$ iteratively for $1000 + \lceil (n+4)/3 \rceil$ times from (x, y, z). Get a real number sequence $\{z_i\}_{i=0}^{n+3}$ by combining the later $\lceil (n+4)/3 \rceil$ approximate states of the Chen system. Generate an 8-bit PRNS $\{x_i\}_{i=0}^{n+3}$ from $\{z_i\}_{i=0}^{n+3}$ by using

$$x_i = \lfloor \mathrm{dec}(|z_i|) \cdot 10^8 \rfloor \bmod 256,$$

  where $|x|$ and $\mathrm{dec}(x)$ return the absolute value and the fractional part of x, respectively.

- *Step (2) Permutation*: Permutate the plaintext sequence $\{p_i\}_{i=1}^{n}$ as described in Sec. 2.3.1 and denote the sequence after permutation with $\{p'_i\}_{i=1}^{n}$, the nonlinear function adopted here is the Logistic map.

- *Step (3) Diffusion*: Given the PRNS $\{x_i\}_{i=0}^{n+3}$, diffuse $\{p'_i\}_{i=1}^{n}$ as described in Sec. 2.3.2 to obtain the ciphertext sequence $\{c_i\}_{i=1}^{n}$.

2.5. Decryption algorithm

The decryption procedures are similar to those of encryption except the following modifications: 1) *Permutation* and *Diffusion* are executed in a reverse order, 2) *Diffusion I* and *Diffusion II* should be executed reversely, 3) Referring to property 1, Eq. (5) and Eq. (6) should be replaced with

$$p_i = \mathrm{eXOR}(m_i \dot{-} \mathrm{eXOR}(m_{i-1}, r'), r)$$

and

$$m_i = \mathrm{eXOR}(c_i \dot{-} \mathrm{eXOR}(c_{i+1}, r'), r),$$

where $a \dot{-} b = (a - b) \bmod 256$.

3. Security and efficiency analysis

3.1. Analysis of key space

It is recommended in [20] that the key space of a chaos-based encryption system should be more than $2^{100} \approx 10^{30}$ to resist the brute-force attack. As described in Sec. 2.4, the secret key of the suggested scheme is the double-precision floating-point representation of the initial condition of the Chen system and the control parameter of the Logistic map, i.e., $\boldsymbol{K} = (x, y, z, \mu)$. The number of significant digits in each parameter is 15, it is concluded that the key space is $(10^{15})^4 = 10^{60}$, which is much larger than the recommended size of a secure cipher.

3.2. Differential analysis

Differential analysis aims to obtain some information of the (equivalent) secret key of an encryption algorithm by means of observing how differences in input can affect the resultant output. To implement the differential analysis in image encryption system, the opponent can encrypt two chosen plain-images with minor modifications, e.g., a slight change of one pixel, then compare the encrypted results. If the minor modification of the plain-image generates significant and unpredictable results in the cipher-image, this attack will become inefficient.

To give a quantitative description of the one-pixel change on the encrypted results, two common measures NPCR (number of pixels change rate) and UACI (unified average changing intensity) are used. They are defined by

$$\mathrm{NPCR} = \sum_{i,j} \frac{D(i,j)}{H \times W} \times 100\%$$

and

$$\mathrm{UACI} = \frac{1}{H \times W} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%,$$

where C_1 and C_2 are two $H \times W$ (height×width) cipher-images corresponding to plain-images differing in one single pixel, $C_1(i,j)/C_2(i,j)$ is the gray-scale value of C_1/C_2 at grid (i,j) and D is a matrix defined by

$$D(i,j) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j), \\ 1, & \text{otherwise.} \end{cases}$$

It is reported in [6] that the expected NPCR and UACI values of a 256 gray-scale image are 99.6094% and 33.4635%, respectively.

The tests of the proposed scheme are carried out as follows. Given a plain-image P_1, randomly choose grid (i,j) and obtain P_2 with

$$P_2(i,j) = \begin{cases} P_1(i,j) + 1, & \text{if } P_1(i,j) < 255, \\ 254, & \text{otherwise.} \end{cases}$$

Encrypt them and denote the cipher-image by C_1 and C_2, then one can calculate NPCR and UACI as described above. Given the secret key $\boldsymbol{K} = (3.0, 4.0, 5.0, 3.999)$, repeat this test 200 times, we found that the mean of NPCR and UACI values are 99.6041% and 33.4198%, respectively, which are very close to their expectation.

3.3. Statistical analysis

3.3.1. Histograms of encrypted images

In Figure 1, we give a typical example of histograms of the plain-image and the corresponding cipher-image. As shown in Fig. 1(d), all the gray-scale values of the cipher-image of "Lenna" are distributed uniformly over the interval $[0, 255]$, which is significantly different from the original distribution shown in Fig. 1(b).

3.3.2. Information entropy

The histogram gives a visual experience of the pixel distribution of cipher-images, while information entropy can offer a measure to quantify the random looking distribution. The most commonly used information entropy is the Shannon entropy [1], which is regarded as the vital feature of randomness. For a message source with 2^N symbols m_i, its Shannon entropy, $H(m)$, is defined as follows:

$$H(m) = -\sum_{i=0}^{2^N-1} Pr(m_i) \cdot \log_2[Pr(m_i)],$$

where $Pr(m_i)$ is the probability of the symbol m_i which is generated by the source. It is easy to prove that a true random gray-scale image with uniformly distributed pixel over the interval $[0, 255]$ can achieve the ideal Shannon entropy 8. Set the secret key $\boldsymbol{K} = (2.0, 3.0, 4.0, 3.9876)$, and get the cipher-image of "Lenna", "Baboon" and "Pepper" of the same size 256×256. The Shannon entropy of the three cipher-images are $H_{\text{Lenna}} = 7.9973$, $H_{\text{Baboon}} = 7.9971$ and $H_{\text{Pepper}} = 7.9969$, which are very close to the ideal value 8.

3.3.3. Correlation of adjacent pixels

The adjacent pixels are strongly correlated is an intrinsic characteristic of digital images without compression. An effective image encryption algorithm should be able to remove this kind of

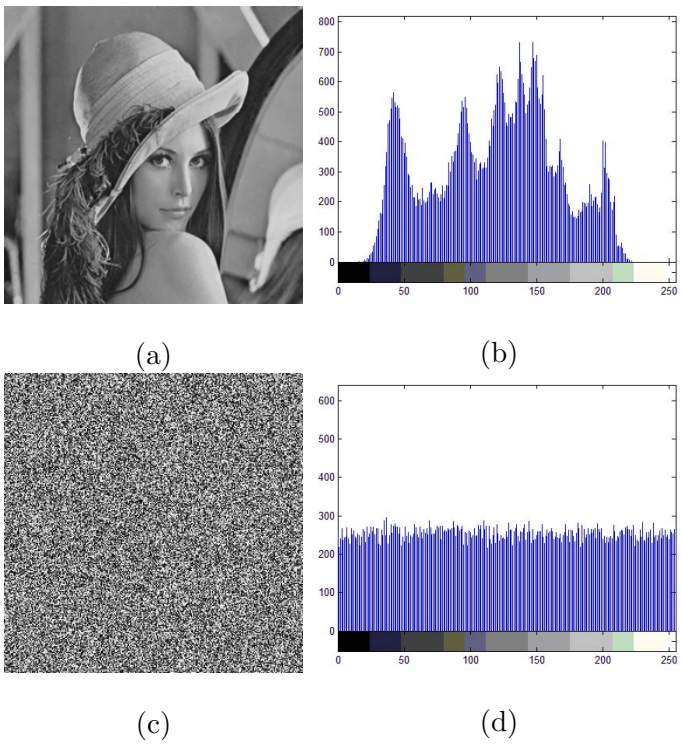

Figure 1: Histograms of plain-image "Lenna" and its corresponding cipher-image: (a) plain-image "Lenna"; (b) Histogram of "Lenna"; (c) the cipher-image of "Lenna"; (d) Histogram of the cipher-image.

relationship. To test the correlation between horizontally adjacent pixels, vertically adjacent pixels and diagonally adjacent pixels, we calculate the correlation coefficient in each direction by

$$cov(x,y) = \frac{\frac{1}{N}\cdot\sum_{i=1}^{N}(x_i-\bar{x})\cdot(y_i-\bar{y})}{\sqrt{(\frac{1}{N}\sum_{i=1}^{N}(x_i-\bar{x})^2)\cdot(\frac{1}{N}\sum_{i=1}^{N}(y_i-\bar{y})^2)}},$$

where $\bar{x} = \frac{1}{N}\cdot\sum_{i=1}^{N}x_i$, $\bar{y} = \frac{1}{N}\cdot\sum_{i=1}^{N}y_i$, (x_i, y_i) is the i-th pair of adjacent pixels in certain direction and N is the total number of the pairs. The result of the correlation coefficients along the three directions of the plain-image "Lenna" and its corresponding cipher-image under secret key $\boldsymbol{K} = (5.0, 3.0, 4.0, 3.999)$ are listed in Table 2. It is clear that the correlation is almost reduced to 0 after encryption.

Table 2: Correlation coefficients between the plain-image "Lenna" and the corresponding cipher-image.

Direction	Plain-image "Lenna"	After encryption
horizontal	0.93903	0.00350
vertical	0.96812	0.00247
diagonal	0.91352	0.00107

3.4. Speed performance

We also test the average encryption (decryption) speed of the proposed scheme on a 3.2GHz Intel Pentium Dual Core CPU with 2GB RAM using VC compiler. Table 3 gives the average speed

of the proposed scheme with respect to images of various size. For comparison, the running speed of the algorithm suggested in [4] and DES are also listed. The results indicate that this scheme is performed in a fast manner.

Table 3: Speed performance of the the proposed scheme, the scheme in [4] and DES algorithm.

Image size (pixels)	The proposed scheme (ms)	The algorithm in [4] (ms)	DES algorithm (ms)
256×256	22	60	28
512×512	98	273	110
1024×1024	415	1180	445

4. Conclusion

This paper presents a simple but secure chaotic cipher for gray images by improving the familiar permutation-diffusion structure. As the plaintext feedback technique is used during permutation, one can develop different permutation sequences for different plain-images, which makes the scheme immune to known/chosen plaintext attack. The diffusion procedure improves the traditional diffusion procedure by employing a nonlinear operator eXOR and generating equivalent key stream dynamically. Experimental tests demonstrate that the scheme owns large key space, high security and good encryption (decryption) speed. Thus, it is a good candidate for real-time image encryption application.

Acknowledgement

This research was supported by the technology project of State Grid of China (No. XX17201200048).

References

References

[1] C. E. Shannon, Communication theory of secrecy systems, Bell System Technical Journal 28 (4) (1949) 656–715.
[2] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, International Journal of Bifurcation and Chaos 8 (6) (1998) 1259–1284.
[3] G. Jakimoski, L. Kocarev, Chaos and cryptography: block encryption ciphers based on chaotic maps, IEEE Transactions on Circuits and Systems I-Regular Papers 48 (2) (2001) 163–169.
[4] G. Chen, Y. Mao, C. K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solitons & Fractals 21 (3) (2004) 749–761.
[5] Y. Zhang, Y. Wang, X. Shen, A chaos-based image encryption algorithm using alternate structure, Science in China Series F-Information Sciences 50 (3) (2007) 334–341.
[6] C. Zhu, A novel image encryption scheme based on improved hyper-chaotic sequences, Optics Communications 285 (1) (2012) 29–37.
[7] M. Francois, T. Grosges, A new image encryption scheme based on a chaotic function, Signal Processing: Image Communication 27 (3) (2012) 249–259.
[8] Y. Mao, G. Chen, S. Lian, A novel fast image encryption scheme based on 3D chaotic baker maps, International Journal of Bifurcation and Chaos 14 (10) (2004) 3613–3624.
[9] C. Huang, H. Nien, Multi chaotic systems based pixel shuffle for image encryption, Optics Communications 282 (11) (2009) 2123–2127.
[10] V. Patidar, N. Pareek, K. Sud, Modified substitution-diffusion image cipher using chaotic standard and logistic maps, Communications in Nonlinear Science and Numerical Simulation 14 (7) (2010) 2755–2765.

[11] G. Àlvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of dynamic lookup table based chaotic cryptosystems, Physics Letters A 326 (3-4) (2004) 211–218.
[12] E. Solak, C. Cokal, O. T. Yildiz, T. Biyikoglu, Cryptanalysis of Fridrich's chaotic image encryption, International Journal of Bifurcation and Chaos 20 (5) (2010) 1405–1413.
[13] C. Li, K. Lo, Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, Signal Processing 91 (4) (2011) 949–954.
[14] L. Y. Zhang, C. Li, K. W. Wong, S. Shu, G. Chen, Cryptanalyzing a chaos-based image encryption algorithm using alternate structure, Journal of Systems and Software 85 (9) (2012) 2077–2085.
[15] C. Li, L. Y. Zhang, R. Ou, K. W. Wong, Breaking a novel colour image encryption algorithm based on chaos, Nonlinear Dynamics 70 (4) (2012) 2383–2388.
[16] Y. Chen, X. F. Liao, K. W. Wong, Chosen plaintext attack on a cryptosystem with discretized skew tent map, IEEE Transactions on Circuits and Systems II-Express Briefs 53 (7) (2006) 527–529.
[17] S. Li, C. Li, G. Chen, N. Bourbakis, K. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, Signal Processing: Image Communication 23 (3) (2008) 212–223.
[18] C. Li, S. Li, K. Lo, Breaking a modified substitution-diffusion image cipher based on chaotic standard and logistic maps, Communications in Nonlinear Science and Numerical Simulation 16 (2) (2011) 837–843.
[19] X. Lai, Defining cryptography, 2nd Workshop on International View of the State-of-the-Art of Cryptography and Security and its Use in Practice, Beijing, 2012.
[20] G. Àlvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, International Journal of Bifurcation and Chaos 16 (8) (2006) 2129–2151.
[21] C. Li, G. Chen, On the security of a class of image encryption schemes, In Proceedings of 2008 IEEE International Symposium on Circuits and Systems (2008) 3290–3293.
[22] X. He, Q. Zhu, P. Gu, A new chaos-based encryption method for color image, Lecture Notes in Artificial Intelligence 4062 (2006) 671–678.
[23] M. Andrecut, Logistic map as a random number generator, International Journal of Modern Physics B 12 (9) (1998) 921–930.